Overseas Security Advisory Council - Global Security News & Reports

# Protecting Intellectual Property in China

## GLOBAL SECURITY CONCERNS

**East Asia / Pacific - China**
13 Jun 2007

### Executive Summary

According to most companies interviewed by OSAC in the past year, the biggest security challenge for firms operating in China is intellectual property (IP) infringement. Specific problems in China related to this topic range a number of different categories, including threats represented by insider informants, economic espionage, counterfeiting, and a legal framework that has yet to catch up with the needs of IP rights enforcement in China. Precisely because IP security is a multi-faceted problem, threat mitigation and response calls for a multi-functional coordinated effort by companies.

*The pdf version of this report may be accessed by clicking on the link on the right hand side of this webpage.*

### Cross-Department Coordination – The Key to IP Security

The impact of intellectual property (IP) infringement on firms cuts across many functional departments. For instance, several of the functions associated with prevention and reaction must be conducted by the firm's legal branch or intellectual property specialists. However, the prevention of mishandling or misuse of IP is typically left up to security personnel, as are investigations of infringement cases. Still, other elements of a comprehensive IP security strategy could also incorporate other departments such as production and business development.

For these reasons, a comprehensive approach to IP security must start with a **cross-department working group** . At a minimum, the group would include representatives from legal and security departments, but depending on the firm, additional representatives from other functional departments could be included as well. For example, in cases where counterfeiting is a concern, production representatives are needed to provide input on how to engineer production processes that are difficult to replicate, trademark lawyers may look at different branding approaches, security officials may look at improving brand identification forensics, while production and logistics may try to tighten supply and distribution chains.

The working group would have under its purview the following responsibilities:

- Creation of a formalized IP security strategy;
- Oversight of strategy implementation and progress;
- Composition of a model response strategy to deal with infringement cases;
- Oversight of infringement cases and disputes;

• Conduct of audits and lessons learned exercises;

All these functions lend themselves to a cyclical and evolutionary approach to IP security which would allow the working group to constantly adapt to new or unforeseen challenges in IP security by implementing reaction plans, resolving disputes, conducting lessons learned exercises, and incorporating new elements into prevention and security planning, as illustrated in the diagram below.

chart

## Components of an IP Security Strategy

Besides assisting to create a baseline for IP security strategy, the practices suggested below will help organizations identify which functional departments to include in the IP security working group. While some practices are clearly responsibilities of security or legal departments, other practices listed below inherently suggest the inclusion into the working group of departments such production, logistics, business development and others.

*Prevention*

• Carefully **vet joint venture partners**. Also consider that prospective partners who have their own reputations to protect are more likely to take an interest in IP security.
• Conduct **due diligence** on suppliers, distributors, and all other local entities that impact on operations.
• **Be critical about what technology is introduced** into China. Attempt to keep new or cutting edge technology development in more secure locations.
• Conduct **background checks** for hires in sensitive positions. Checks should be conducted not only on individuals who will be utilizing and manipulating data, but also on **technical personnel** maintaining the servers and networks where information is stored and transmitted.
• Incorporate IP protections such as **non-disclosure and non-compete provisions** into all contracts with direct-hire personnel and business partners. These provisions may need to be adapted from U.S .models in order to be consistent with Chinese law to be effective.
• **Manage relationships with distributors and suppliers** through multiple people to lessen opportunities for collusion.
• Design and **compartmentalize production** processes and production equipment so that they are difficult to replicate.
• **Encrypt** all laptops, mobile devices, etc., that may be used for travel overseas.
• **Register patents, trademarks, domain names and other IP rights** (*See guidance on registering IP here*). Also create and register **Chinese-language equivalents for trademarks**. In cases where firms failed to create local language trademarks, the market created or imposed local language equivalents that were then registered by a hostile entity.

*Enforcement & Being Proactive*

• **Collaborate** with other companies to investigate specific counterfeit operations. Collaboration will improve the effectiveness of investigations as well as deterrence by improving evidence gathering and enabling local law enforcement to better satisfy high Chinese conviction thresholds.
• While remaining in compliance with the Foreign Corrupt Practices Act and other laws, develop relationships with local officials in government offices that have a bearing on IP security and enforcement. The development of such relationships, known in China as "**guanxi**," is a pivotal component of Chinese society. The development of guanxi can take years of careful attention and maintenance. In certain instances, the U.S. Embassy can also provide support by making inquiries into the status of specific infringement cases.
• Create **unique product packaging details** that will help in identifying counterfeit goods. Adjustments to packaging features, including holograms and small variations in color from one country to another, also make products harder to replicate faithfully.
• Attend **trade fairs** such as the China Import and Export Fair, otherwise known as the "Canton Fair," to detect possible counterfeits. The Canton Fair also has an IP complaint center.
• Formulate a **model reaction plan** to deal with cases of infringement. Firms hoping to formulate an effective reaction plan should be familiar with the enforcement options in China, including administrative, civil, criminal and other options available through Chinese Customs. For more information on these enforcement options, please refer to the IPR Toolkit available on U.S. Embassy Beijing's website. When formulating a reaction plan (and executing enforcement in infringement cases), firms should also seek out qualified Chinese legal counsel. China's State Intellectual Property Office maintains a list of PRC-government authorized patent and trademark agents, and the U.S. Commercial Service publishes a list of consulting and law firms in *Contact China: A Resource for Doing Business in People's Republic of China*. Also view a list of law offices on the Beijing and Shanghai Embassy websites.

*Education*

• Equip local Chinese employees with a structured **IP security education**. This could mean periodic **briefings** as well as the use of a public **awareness campaign**. For example, a campaign may be used to expand employees' awareness of **economic espionage** and key behavioral patterns of insider informants. One low-maintenance element of such a campaign could be the use of **posters** in the workplace (*For resources on economic espionage visit the OSAC Resource Library*).
• Try to instill a **sense of company ownership and loyalty** in staff. This might be accomplished through team development exercises, or by instilling local Chinese hires with more responsibility. In some cases, this may mean slowly phasing out the presence of expatriate staff. Companies have expressed that in operations where local nationals are allowed to ascend to management and leadership positions, staff loyalty has increased, helping to **mitigate the threat of insider informants**. One outgrowth of staff outreach and awareness campaigns could be the promotion of an internal, anonymous **fraud hotline**.
• Identify critical IP threat countries such as China and require **travelers** to these locations to obtain briefings on economic espionage and travel security ( *See counterintelligence guidance for travelers here*).

*Audits & Monitoring*

• Conduct periodic **audits of IP security protocols** and internal controls to ensure that policies set forth by the IP security working groups are being implemented. This activity should be directed by the working group.
• Create a mechanism to **monitor the marketplace** for patent (counterfeiting), copyright (piracy), or trademark infringement, as well as trade secret theft. Record the incidence or presence of infringement.
• As a part of a market entry strategy, **monitor trademarks registered** with countries of interest to ensure that local hostile entities do not preemptively register your company's trademark (*Many companies hire local law firms or trademark and patent agents to conduct these activities*).

*Controls*

• Create a **formal classification scheme for IP** according to information sensitivity levels. Identify who has access to what levels of classified information. Special access areas where highly sensitive information is processed can be placed off limits to improperly cleared personnel. **Physical access** to such spaces may be limited to authorized personnel through the use of **programmable access badges**. Practice strong **information control** and operate on a "need to know" basis. Institute "clean desk" policies and use shredders.
• Take an **inventory** of where sensitive IP is stored, including servers, mobile devices, storage media and networks.
• **Track dataflows** for abnormalities.
• Restrict and **monitor movement of mobile devices** and information storage media from facilities.

## Conclusion

IP security in China in many cases relates to the protection of information in its purest form. This is why many companies are preoccupied with threats related to insider informants and economic espionage. Another part of battling IP infringement in China is investigating and stopping active counterfeit operations. However, taking a broader view of problems associated with IP protection, one sees many threats of different varieties. In regions outside of East Asia, OSAC constituents have reported that some of their biggest concerns related to IP protection deals with cargo theft. In other cases, companies deal with a profusion of cyber crimes conducted through spam email and "dummy" websites meant to extract sensitive information from clients, putting valuable customers at risk. Furthermore, companies deal with many other different threats that impact IP security directly. The fact that IP infringement represents so many different threats affecting a variety of functional departments in any one company only reinforces the need for a coordinated, multi-functional mitigation and response strategy. Furthermore, such a multi-functional capacity in companies increases coordination on other issues, generating more resiliency to other threats and challenges.

Overseas Security Advisory Council • Bureau of Diplomatic Security
U.S. Department of State • Washington, D.C. 20522-2008
Telephone: 571-345-2223 • Facsimile: 571-345-2238
Contact OSAC Webmaster